EXHIBIT A

PIERCE O'DONNELL (SBN 081298)
PODonnell@GreenbergGlusker.com
TIMOTHY J. TOOHEY (SBN 140117)
TToohey@GreenbergGlusker.com
PAUL BLECHNER (SBN159514)
PBlechner@GreenbergGlusker.com
GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
2049 Century Park East, Suite 2600
Los Angeles, California 90067Telephone:
310.553.3610
Fax: 310.553.0687

Attorneys for Plaintiff
MICHAEL TERPIN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MICHAEL TERPIN,

Plaintiff,

v.

AT&T Mobility, LLC; and DOES 1-25,

Defendants.

Case No. 2:18-cv-6975-ODW-KS

SECOND AMENDED COMPLAINT FOR:

(1) DECLARATORY RELIEF: UNENFORCEABILITY OF AT&T CONSUMER AGREEMENT AS UNCONSCIONABLE AND CONTRARY TO PUBLIC POLICY; (2) UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION, FEDERAL COMMUNICATIONS ACT, 47 U.S.C. §§ 206, 222; (3) DECEIT BY CONCEALMENT, CAL. CIV. CODE §§ 1709, 1710; (4) MISREPRESENTATION; (5) NEGLIGENCE; (6) NEGLIGENT SUPERVISION AND TRAINING; (7) NEGLIGENT HIRING; and (8) BREACH OF CONTRACT—AT&T PRIVACY POLICY

DEMAND FOR JURY TRIAL

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Plaintiff Michael Terpin, by and through his counsel, complains and alleges as his Second Amended Complaint as follows against AT&T Mobility, LLC ("AT&T"):

JURISDICTION AND VENUE

1. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts. The Court also has jurisdiction over this matter under 28 U.S.C. § 1332 in that the amount in controversy exceeds $75,000 and Plaintiff and Defendants are citizens of different states in that Plaintiff, Michael Terpin is domiciled in Puerto Rico with a residence in California, and Defendants AT&T, Inc. and AT&T Mobility, Inc., are corporations with their principal places of business, respectively, in Texas and Georgia.

2. Venue is proper in this Court under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c) and (d) because a substantial part of the events or omissions giving rise to this Complaint occurred in this District. Plaintiff Michael Terpin has a residence in Los Angeles County, California. Mr. Terpin obtained wireless services from AT&T in Los Angeles County in or about the mid-1990's. AT&T does business in and is subject to the Court's jurisdiction in this District. AT&T's violation of Mr. Terpin's privacy in those services is the subject of this complaint. Mr. Terpin continued at all times relevant to the allegations herein to receive wireless services from AT&T for a telephone number with a Southern Californian area code.

INTRODUCTION

3. AT&T solemnly promises its cellular telephone subscribers that it will safeguard their private information—and particularly their data-rich SIM cards—from any unauthorized disclosure. Besides the numerous promises that AT&T makes in its own Privacy Policy and Code of Business Conduct, federal and

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

state law impose a strict duty on the nation's second largest cellular telephone carrier to take all necessary steps to preserve the privacy of its almost 140 million customers. In AT&T's case, this mandate has fallen on deaf ears.

4. In one notorious instance, AT&T employees were found culpable for stealing personal information for over 200,000 customers and selling it to criminals to unlock mobile phones. This massive security failure prompted the Federal Communications Commission to levy a record fine of $25 million and secure a Consent Decree requiring AT&T to implement detailed measures to enhance its subscribers' protection against unauthorized disclosures of their private information. AT&T did not learn its lesson.

5. More recently, AT&T employees, as has been widely reported by law enforcement, are participating in a new species of fraud—SIM swap fraud—which is a metastasizing cancer attacking AT&T customers and allowing hackers readily to bypass AT&T security to rob AT&T customers of valuable personal information and millions of dollars of cryptocurrency.

6. A "SIM swap" is a practice whereby a hacker gains access to a victim's telephone account or number in order to intercept communications, including text messages, to the mobile telephone. A perpetrator of a SIM swap typically arranges through bribery of someone with access to customer information to change the SIM card assigned to a user to a telephone under the control of the hacker or the hacker's accomplices. Once the SIM transfer has occurred, the hacker uses the hacker's phone which contains a SIM card associated with the victim's account to impersonate the victim with service providers, such as e-mail providers, and uses the victim's phone number to request changes to account settings and to reset passwords to take control of the victim's accounts and private information. This is a direct, intentional form of theft, similar to stealing the key to a car (the key is not the car itself, but it directly enables the theft of the car without the owner's permission). The sole reason for these bribes is the enabling of thieves to hack into

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

bank accounts, credit card records and digital assets, including cryptocurrency, stored in digital wallets that would not have otherwise been accessible without the theft of the digital identity "key" found in the SIM.

7. Since the SIM swap described herein, AT&T has done virtually nothing to prevent ongoing SIM swap frauds. As a result, there have been hundreds of millions of dollars in subsequent direct losses by its customers of assets allegedly "protected" by this authentication scheme promoted by AT&T to its users and to software providers as providing additional safety. Even after learning of the complicity of its employees from law enforcement, AT&T has continued not to supervise low-level clerks to prevent them from turning over the digital "keys" of its customers' accounts to hackers.

8. AT&T's subscriber privacy protection system is thus a veritable modern-day Maginot Line: a lot of reassuring words that promote a false sense of security whereas AT&T knows that hackers are readily able to bypass its weak security by co-opting AT&T's own employees. AT&T persists in not providing adequate security or providing security that is easily evaded by hackers and/or its own employees even though it knows that hackers target its systems because the hackers know they are riddled with flaws. Most troubling, AT&T has not improved its protections even though it knows from numerous incidents that some of its employees actively cooperate with hackers in SIM swap frauds by giving hackers direct access to customer information and by overriding AT&T's security procedures. On information and belief, Jahmil Smith, the AT&T agent involved in Mr. Terpin's hack, was bribed by a criminal gang in order to allow the hackers access to the "private keys" to cryptocurrency assets that otherwise would be unavailable to them.

9. In recent incidents, including incidents that have led to criminal complaints against individuals involved in SIM swaps, including AT&T employees, law enforcement has even confirmed that AT&T employees profited

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

from bribes for working directly with cyber terrorists and thieves in SIM swap frauds. Such was the case regarding two AT&T contract employees in Tucson, Jarratt White and Robert Jack, who facilitated 41 SIM swaps in the single month of May 2018 for a total bribe from the hackers of $4,300 that resulted in the theft of approximately $2,143,471.59. *See* Exhibit F (Criminal Complaint in *United States v. White*).

10. The porosity of AT&T's privacy program is dramatically evident in this case, which follows a pattern well known to AT&T and which has been repeated on countless times before and after the events that befell Mr. Terpin. An experienced, high profile cryptocurrency investor, Plaintiff Michael Terpin was a longtime AT&T subscriber who entrusted his sensitive private information to AT&T and relied on AT&T's assurances and its compliance with applicable laws. Given all the carrier's hype about protecting customer security, Plaintiff believed that it would keep its promises about absolutely safeguarding him from a data breach that could lead to the theft of tens of millions of dollars of cryptocurrency. In reality, however, Plaintiff was victimized by not one, but two hacks within seven months.

11. On information and belief Terpin further alleges that even after AT&T had placed vaunted additional protection on his account after an earlier hacking incident, an AT&T retail clerk (Jahmil Smith) was easily able to fabricate information indicating that Mr. Terpin visited the store and showed identification when in fact Mr. Terpin did not visit the store. Smith then transferred the key to the digital identity of Mr. Terpin in the SIM for his telephone account to an eager gang of hackers.

12. Importantly, the precise mechanics of that hack are best known by the hackers. Upon information and belief, Terpin alleges that the AT&T employee's cooperation allowed a criminal gang to use their control of Mr. Terpin's telephone account to intercept communications, including text messages, to reset

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

passwords for Mr. Terpin's accounts and to access files under those accounts containing confidential information used to access cryptocurrency wallets and/or exchanges. This system long promoted by AT&T and other phone companies is called "two factor authentication" in that it provides a second factor to prove identity to access a protected software account (the first factor is typically an email address and/or a password). Once the perpetrators gained unauthorized access to the wallets, they transferred Mr. Terpin's cryptocurrency to wallets and/or accounts controlled by the perpetrator(s). In the case of Mr. Terpin, Mr. Terpin is informed and believes that the hackers intercepted 2FA messages to a phone under their control with Mr. Terpin's AT&T account to gain access to deleted files and fragments accessible by hackers through sophisticated techniques on a password-protected cloud that contained confidential information that allowed them to gain access to Mr. Terpin's electronic wallets holding almost $24 million of cryptocurrency. Put simply, the SIM was an absolutely necessary component of the hack, without which the cryptocurrency could never have been accessed, much less stolen.

13. Although AT&T's privacy and security officers were well aware of the porosity of its protections of its customers' personal information, AT&T provided hackers with access to Mr. Terpin's telephone account through enabling its employees and agents the unfettered ability to falsify records and transfer the SIM to a phone under their control, without adhering to its security procedures, that allowed the cryptocurrency theft to occur by allowing the hackers to take possession of Mr. Terpin's account and digital identity to intercept 2FA messages. What AT&T did was like a hotel giving a thief with a fake ID a room key *and* a key to the room safe to steal jewelry in the safe from the rightful owner, or, even worse, simply handing over the same keys to a known impostor when someone slipped them a $20 bill.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

14. Since the hack to Mr. Terpin has occurred and this lawsuit has been filed, he has been contacted by more than 50 SIM swap victims of AT&T, including many who had cryptocurrency stolen under nearly identical circumstances. Cryptocurrency investors are particularly vulnerable because cryptocurrency transfers cannot be reversed. AT&T's failure to protect cryptocurrency investors is thus undermining the stability of transactions in this important new $300 billion marketplace. Moreover, AT&T's stubborn refusal to implement relatively easy fixes to its security system—despite the myriad of complaints, news stories, and incidents of fraud—has laid bare the fact that the telecommunication provider's failure to guard against criminals working in their retail stores is the weak link of the 2FA security system.

15. AT&T is doing virtually nothing to protect its almost 140 million customers from SIM card fraud and the subsequent theft of assets that AT&T promised to protect through its 2FA system (in particular, through its higher level of protection that it promised Mr. Terpin) that follows as surely as night follows day. AT&T is therefore directly culpable for these attacks because it is well aware that hackers are readily able to avoid its security protections to subject its customers to SIM swap fraud and that such hackers rely on such fraud and theft to obtain 2FA communications that lead them directly to customers' private communications and valuable digital assets. AT&T does almost nothing to protect its customers from such fraud because it has become too big to care. Indeed, AT&T has sacrificed its customers for its own financial gain because it is unwilling to install basic security precautions for preventing its employees to fraudulently transfer a SIM card to a criminal gang--something that law enforcement statistics show has happened very frequently to AT&T, with many more thefts unreported.

16. This lawsuit seeks to hold AT&T accountable for its abject failure to protect subscribers like Mr. Terpin from the theft of protection to their digital identity by its own employees. Apparently, AT&T preferred to buy Time

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Warner for over $85 billion than pay for a state-of-the art security system and hire, train, and supervise competent and ethical employees—even when it was well known to AT&T that its system was vulnerable to precisely the type of hack experienced by Mr. Terpin. Indeed, AT&T knew that Mr. Terpin himself has previously been subject to SIM swap fraud. And, Mr. Terpin is informed and believes that AT&T further knew that SIM swapping fraud has become more and more prevalent as a gateway to the access of customers' accounts, resulting in a wide variety of harms including, as was the case with Mr. Terpin, the theft of cryptocurrencies.

17. On information and belief, law enforcement has approached AT&T frequently to ask for satellite records as evidence of whether and when a SIM transfer has occurred and whether it occurred in a store, as noted in the AT&T transaction log, or whether the transfer occurred hundreds of miles away by a hacker. After this many thefts and subpoenas by law enforcement, AT&T cannot proclaim that it lacks knowledge of the crimes being committed by its own employees and agents due to its lax security practices. A verdict for $24 million of compensatory damages and over $200 million for punitive damages might attract the attention of AT&T's senior management who have long ignored this practice so that they will spend serious money on an acceptable customer protection program and measures to ensure that its own employees are not complicit in theft and fraud. Then and only then will AT&T's promise to protect the types of personal information that directly led to the hacking of Mr. Terpin's accounts ring true.

THE PARTIES

18. Mr. Terpin is well known for his involvement with cryptocurrency. Cryptocurrency (also known as "crypto") is digital or virtual currency used as a medium of exchange, store of value, and hedge against other investment assets such as stocks and bonds. that uses cryptography to secure the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

transaction. Typically, the holder of cryptocurrency has both a "public" and a "private" key or address that the holder uses to receive, transfer, use or store cryptocurrency. The private key, which is under the control of the owner of the cryptocurrency, is used to write in a public ledger to transfer cryptocurrency but is not displayed publicly. The private key is a cryptographically secure series of letters and numbers, which is typically filed in a "wallet." Because the key can be used to "spend" cryptocurrency, owners of cryptocurrency typically keep such keys secure. Cryptocurrency is decentralized, operates independently of a central bank, and is often traded by parties through "exchanges." The total market value of all cryptocurrency exceeded $800 Billion on the day of Mr. Terpin's theft.

19. Mr. Terpin is a prominent member of the blockchain and cryptocurrency community. In 2013, he started BitAngels, the first angel group for investing in bitcoin and blockchain companies, and CoinAgenda, the first high-end investor series for family offices and funds investing in digital assets. Mr. Terpin also runs Transform Group, the preeminent public relations and advisory firm in the cryptocurrency and blockchain sectors. Like others in the blockchain community, Mr. Terpin is a high-profile hacker target because of his publicized involvement in cryptocurrency enterprises.

20. AT&T, Inc. is a Delaware Corporation with its principal place of business in Dallas, Texas. Defendant AT&T Mobility, LLC ("AT&T Mobility"), which is marketed as "AT&T," is a wholly-owned subsidiary of AT&T, Inc. with its principal place of business in Brookhaven, Georgia. AT&T Mobility provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands. AT&T Mobility is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq.* AT&T Mobility is regulated by the Federal Communications Commission ("FCC") for its acts and practices, including those occurring in this District. AT&T, Inc. and AT&T Mobility are herein referred to collectively as "AT&T."

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

21. Defendant AT&T Mobility is the second largest wireless provider in the United States with 138.8 million subscribers as of the third quarter of 2017. AT&T, Inc., as it is presently constituted, is the result of the recombination of many of the companies split off from the original AT&T (also known as "The Telephone Company" or "Ma Bell.") AT&T, Inc. is a behemoth which, in 2017, had operating revenues of over $160 billion and assets of over $444 billion.

22. Over the past decade, AT&T has gone on a buying spree costing over $150 billion, acquiring: Bell South (including Cingular Wireless and Yellowpages.com), Dobson Communications, Edge Wireless, Cellular One, Centennial, Wayport, Qualcomm Spectrum, Leap Wireless, DirecTV, and Iusacell and NII Holdings (now AT&T Mexico). During the same period, AT&T's mobile phone business was rated as the worst among major providers. *Consumer Reports* named it the "worst carrier" in 2010, and the next year, J.D. Power found AT&T's network the least reliable in the country—a dubious achievement that it also earned in prior years. Little wonder that its customers were the least happy of subscribers of the Big Four carriers according to the American Consumer Index. In the meantime, AT&T has purchased for a total equity value of $85.4 billion Time Warner Inc.—the owner of HBO, Warner Bros, CNN, Turner Broadcasting, Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

23. According to media reports, AT&T mobile telephone customers have been the subject of more privacy violations than subscribers to other cell phone companies. The Electronic Frontier Foundation has recently called out AT&T's "hypocrisy" in calling for an "Internet Bill of Rights" when in fact "few companies have done more to combat privacy and network neutrality than AT&T." https://www.eff.org/deeplinks/2018/01/hypocrisy-atts-internet-bill-rights AT&T has even lobbied the FCC to stop applying the privacy provisions of the FCA to its broadband services, while arguing (unsuccessfully) that it was not subject to the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

jurisdiction of the Federal Trade Commission ("FTC") to govern privacy and data security pursuant to its jurisdiction to regulate unfair and deceptive acts under Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1)(2).

24. As further detailed below, AT&T has also been and continues to be subject to numerous incidents of SIM card swap fraud, including incidents involving prominent members of the cryptocurrency community. It is further aware that its employees are complicit in such fraud and can bypass AT&T's security concerns. Indeed, a growing number of its employees and/or agents have been charged in criminal cases for participating in SIM swap fraud and their involvement in such fraud has been highlighted by law enforcement authorities. And, plaintiff is informed and believes that AT&T has knowledge of the involvement of a growing number of employees and/or agents in such incidents. Despite the incidents, AT&T persists in not securing its system against a cresting wave of such fraudulent activity.

25. Since Mr. Terpin's hack occurred, AT&T customers continue to be subject to widespread SIM swap fraud. On information and belief, AT&T's response to complaints about these hacks has been brusque, if not callous. AT&T has made it virtually impossible for customers to contact its fraud department, refused to provide even basic information about the SIM swaps, has denied knowledge of the hacks, and has even flatly told customers that it has no intent of investigating the involvement of its own employees in such frauds. Even though, on information and belief, AT&T has a portal to directly report suspect incidents to the FCC, it has denied the applicability of the privacy provisions of the FCA to hacks even when hackers have taken entire control of a customer's phone.

26. Given AT&T's dismal track record on consumer privacy, including the FCC's fine and Consent Decree referenced below and its failure to prevent fraud of the sort that victimized Mr. Terpin, it ought to have invested its money and attention to protecting its cellular telephone subscribers from the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

onslaught of hacking and insider data breaches before it spent billions of dollars for new companies, like Time Warner. After all, AT&T was historically a *telephone* company.

27. Plaintiff is ignorant of the true names or capacities of the defendants sued herein under the fictitious names DOES ONE through TWENTY-FIVE inclusive. Plaintiff further alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, proximately caused plaintiff's damages, and was acting as agent for the others.

FACTUAL ALLEGATIONS

AT&T'S STATUTORY OBLIGATION TO PROTECT CUSTOMERS' PERSONAL INFORMATION UNDER THE FEDERAL COMMUNICATIONS ACT

28. As a common carrier, AT&T is obligated to protect the confidential personal information of its customers under Section 222 of the FCA, 47 U.S.C. § 222.

29. Section 222(a), 47 U.S.C. § 222(a), provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers . . .." The "confidential proprietary information" referred to in Section 222(a), is abbreviated herein as "CPI."

30. Section 222(c), 47 U.S.C. § 222(c), additionally provides that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

directories." The "customer proprietary network information" referred to in Section 222(c) is abbreviated herein as "CPNI."

31. Section 222(h)(1), 47 U.S.C. § 222(h)(1), defines CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that term does not include subscriber list information."

32. The FCC has promulgated rules to implement Section 222 "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." *See* 47 CFR § 64.2001 *et seq.* ("CPNI Rules"); *CPNI Order*, 13 FCC Rcd. at 8195 ¶ 193. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. 47 CFR § 64.2005.

33. The CPNI Rules require carriers to implement safeguards to protect customers' CPNI. These safeguards include: (i) training personnel "as to when they are and are not authorized to use CPNI"; (ii) establishing "a supervisory review process regarding carrier compliance with the rules;" and (iii) filing annual compliance certificates with the FCC. 47 CFR § 64.2009(b), (d), and (e).

34. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. 47 CFR § 64.2010. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 CFR § 64.2010(a). Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

visit." *Id.* In the case of in-store access to CPNI, "[a] telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, *first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information*." 47 CFR § 64.2010(d) (emphasis added). "Valid photo ID" is defined in 47 CFR § 64.2003(r) as "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired."

35. The FCC has determined that information obtained from customers through a common social engineering ploy known as "pretexting" is CPNI. *See In the Matter of Implementation of the Telecommunications Acts of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd. 6927 (2007) ("Pretexting Order"). Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." *Id.*, n. 1. Such "call detail" and "private communications" are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.* The FCC concluded that "pretexters have been successful at gaining unauthorized access to CPNI" and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI." *Id.* at 6933. The FCC modified its rules to impose additional security for carriers' disclosure of CPNI and to require that law enforcement and customers be notified of security breaches involving CPNI. *Id.* at 6936-62.

36. In its Pretexting Order, the FCC stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information." *Id.* at 6959, ¶ 64. The FCC further stated that "[w]e decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization." *Id.* at 6960,

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

¶ 66. In a statement directly relevant to the facts alleged below, the FCC also stressed the fact that *someone having obtained information fraudulently is strong evidence of the carrier's failure to satisfy the requirements of section 222*. The FCC stated that "we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable *in light of the threat posed* by pretexting and the *sensitivity of the customer information at issue*." *Id*. at 6959, ¶ 63 (emphasis added).

37. As further alleged below, AT&T violated Section 222 of the FCA and the CPNI Rules and ignored the warning in the Pretexting Order on January 7, 2018 when its employees provided hackers with Mr. Terpin's SIM cards containing or allowing access to Mr. Terpin's personal information, including CPI and CPNI, without Mr. Terpin's authorization or permission, and without requiring that the individual accessing Mr. Terpin's account present valid identification or comply with AT&T's own procedures.

38. Despite its statutory duties to protect the privacy of AT&T's customers, the FCC, under its current "business friendly" leadership, has not made any response to the ongoing plague of SIM swap cases. Mr. Terpin's lawsuit thus fulfills a valuable public function of publicizing the complicity of AT&T in SIM swaps and its refusal to take even elementary measures to protect the privacy of its own customers.

AT&T EMPLOYEES' DISCLOSURE OF CUSTOMERS' PERSONAL INFORMATION AND THE APRIL 8, 2015 FCC CONSENT DECREE

39. On April 8, 2015, the FCC fined AT&T a record $25 million for violating Section 222 of the FCA by allowing its employees to hand over to thieves the CPNI of almost 280,000 customers. In addition to being forced to pay $25

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

million to the FCC, AT&T entered into a consent decree requiring it to implement measures to protect CPNI. The April 8, 2015 consent decree ("Consent Decree") remains in full force and effect.

40. In the Consent Decree and the FCC's adopting order ("Adopting Order"), the FCC highlights AT&T's lax security practices and dismal failure to supervise and monitor employees that led to its unprecedented breach of its customers' confidential and private information. *See In the Matter of AT&T Services, Inc.*, 30 FCC Rcd. 2808 (April 8, 2015 Adopting Order and Consent Decree) (attached hereto as Exhibit A).

41. The FCC investigation revealed that numerous AT&T call center employees provided the CPNI of hundreds of thousands of customers, including names, phone numbers and Social Security Numbers to unauthorized third parties, who used this information to gain access to unlock codes for mobile telephones and to remove territorial and network restrictions. *Id*. at 2808. The investigation further revealed that employees were frequently paid by criminals to hand over AT&T customers' personal sensitive information, including account-related CPNI. *Id*. at 2808, 2813-15.

42. The FCC found that AT&T employees used their login credentials to access the confidential information of almost 280,000 customers. The FCC concluded that AT&T's data security measures "failed to prevent or timely detect a large and ongoing Data Breach." *Id.* at 2813 (Consent Decree ¶ 8).

43. The FCC also found that AT&T had not properly supervised its employees' access to its customers' personal information, including CPNI. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information and constitutes an unjust and unreasonable practice in violation of the Act." *Id. at* 2808 (Adopting Order § 2).

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

44. In the Adopting Order, the FCC emphasized the importance of AT&T's obligation to adhere to the obligations embodied in Section 222 of the FCA. According to the Adopting Order, the purpose of Section 222 is to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information." *Id*. Carriers like AT&T are thus required to take "'every reasonable precaution' to protect their customers' data" and to notify consumers regarding any breaches in order to "aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected consumers [to] be proactive in protecting themselves in the aftermath of a data breach." *Id*.

45. As a condition of terminating the FCC's investigation of AT&T's violations of Sections 201(b) and 222 of the FCA, the FCC imposed numerous requirements on AT&T to improve its supervision of employees and to adhere to its legal obligation to protect the privacy of AT&T's customers. Moreover, the Consent Decree imposed obligations not only on AT&T itself, but also on AT&T's "Covered Employees," who are defined as "all employees and agents of AT&T who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or Customer Proprietary Network Information at Call Centers managed and operated by AT&T Mobility." *Id.* at 2811. "Call Center" is defined broadly in the Consent Decree as call centers operated by AT&T or its contractors "that provide mobility customer service or wireless sale service for AT&T Mobility consumer customers." *Id*. at 2810.

46. Paragraph 17 of the FCC Consent Decree requires AT&T to designate "a senior corporate manager with the requisite corporate and organization authority to serve as a Compliance Officer . . .." *Id*. at 2816. AT&T's Compliance Officer must be "responsible for developing, implementing, and administering the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Compliance Plan and ensuring that AT&T complies with the terms and conditions of the Compliance Plan and this Consent Decree." *Id.*

47. Paragraph 18 of the FCC Consent Decree requires AT&T to institute a "Compliance Plan designed to ensure future compliance with the [FCA] and with the terms and conditions of this Consent Decree." *Id.* The Compliance Plan must include a Risk Assessment, Information Security Program, Ongoing Monitoring and Improvement, and a Compliance Review. *Id.*

48. The "Information Security Program" required in Paragraph 18(b) must be "reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees . . .." *Id.* AT&T's program must be documented in writing and include:

> (i) administrative, technical, and physical safeguards reasonably designed to protect the security and confidentiality of Personal Information and CPNI;
>
> (ii) reasonable measures to protect Personal Information and CPNI maintained by or made available to Vendors, Covered Employees, and Covered Vendor Employees. . .;
>
> (iii) access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees;
>
> (iv) reasonable processes to assist AT&T in detecting and responding to suspicious or anomalous account activity, including whether by malware or otherwise, involving Covered Employees and Covered Vendor Employees; and
>
> (v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

49. Paragraph 18(c) of the Consent Decree requires AT&T to "monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the [FCA], the CPNI Rules, and this Consent Decree." *Id.* at 2817. In addition, Paragraph 18(g) requires AT&T to "establish and implement a Compliance Training Program [for employees] on compliance with Section 222, the CPNI Rules, and the Operating Procedures." *Id.* All "Covered Employees" are required to be trained within six months of hire and periodically thereafter. *Id.*

50. AT&T must report noncompliance with the terms and conditions of the Consent Decree within fifteen (15) days after discovery of such noncompliance. *Id.* at 2819 (Consent Decree ¶ 20). In addition, "AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual." *Id.* Moreover, AT&T is required to file compliance reports with the FCC six (6) months after the Effective Date, twelve (12) months after the Effective Date, and thirty-six (36) months after the Effective Date." *Id.* (Consent Decree ¶ 21).

51. The provisions in Paragraphs 17 and 18 of the Consent Decree were applicable at all relevant dates to the acts and omissions alleged in this Complaint. *Id.* at 2820 (Consent Decree ¶ 22 (Paragraphs 17-18 expire seven (7) years after the "Effective Date," *i.e.*, April 7, 2022)). As further alleged below, AT&T violated numerous terms of the April 8, 2015 Consent Decree by failing to implement adequate security procedures to protect Mr. Terpin's personal information, including CPNI, by failing to supervise and monitor its employees, by failing to ensure that its employees were ethical and competent, by failing to follow its security procedures and by failing to follow its legal obligations to protect Mr.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Terpin's personal information under the FAC, CPNI Rules, and the Consent Decree. Mr. Terpin alleges on information and belief that AT&T also failed to report to the FCC the two data breaches involving Mr. Terpin, as required by FCC regulations and the Consent Decree. Mr. Terpin further alleges on information and belief that AT&T has failed to report to the FCC numerous additional data breaches involving victims of fraud where AT&T employees provided hackers access AT&T's customers' telephone numbers who stole money from the customers. Mr. Terpin's lawsuit thus serves the valuable function of publicizing AT&T's abject failure to prevent the wholesale theft of its customers' personal information, including the active participation of its own employees in such theft, to prevent future harm to AT&T's customers. It also publicizes AT&T's complicity in the thefts of the information and assets of its own customers.

AT&T'S PRIVACY AND SECURITY COMMITMENTS TO CUSTOMERS IN ITS PRIVACY POLICY AND CODE OF BUSINESS CONDUCT

52. In its Privacy Policy ("Privacy Policy") and Code of Business Conduct ("COBC"), AT&T acknowledges its responsibilities to protect customers' "Personal Information" under the FCA, the CPNI Rules and other regulations. A true and correct copy of the Privacy Policy in effect in January 2018 available at http://about.att.com/sites/privacy_policy is attached hereto as Exhibit B. A true and correct copy of the COBC in effect in January 2018 available at https://ebiznet.sbc.com/attcode/index.cfm is attached hereto as Exhibit C.

53. In its Privacy Policy and COBC, AT&T makes binding promises and commitments to Mr. Terpin, as its customer, that it will protect and secure his "Personal Information." The Privacy Policy defines "Personal Information" as "[i]nformation that identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address." AT&T states that, among the information that it collects from and about its customers, are "your name, address, telephone number, e-mail

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

address" and service-related details such as payment history, security codes, service history and similar information. AT&T also collects information relating to the use of its networks, products and services. "Personal Information" thus includes both CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

54. In its Privacy Policy AT&T promises that it takes its responsibility "to safeguard your [*i.e.*, the customer's] Personal Information seriously" and that it will not share its customers' Personal Information except for legitimate business purposes. It further states that "we will not sell [users'] Personal Information to anyone, for any purpose. Period."

55. AT&T further promises that it has numerous safeguards in place to protect the Personal Information of its customers and makes the following promises to its customers:

> We've worked hard to protect your information. *And we've established electronic and administrative safeguards designed to make the information we collect secure*. Some examples of those safeguards include:
>
> - All of our employees are subject to the AT&T Code of Business Conduct (COBC) (https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal information. Some examples are:
  - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
  - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
  - Limiting access to Personal Information to only those with jobs requiring such access; and
  - *Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information*.

(Emphasis added.)

56. AT&T's COBC also makes binding commitments to Mr. Terpin, as an AT&T customer, that it will protect his Personal Information and that it will adhere to all its legal obligations. Those legal obligations include, by implication, Section 222 of the FCA, the CPNI Rules, and other legal obligations that govern protection of confidential and private information. For example, AT&T's chairman and chief executive, Randall Stephenson, and its chief compliance officer, David Huntley promise that because "[o]ur customers count on us" "[t]hat we will follow not only the letter of the law, but the spirit of the law" and "that we will always take responsibility." *The COBC also specifically promises that AT&T will "protect the privacy of our customers' communications" because "[n]ot only do our customers demand this, but the law requires it.*

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Maintaining the confidentiality of communication is, and always has been, a crucial part of our business." (Emphasis added.)

57. AT&T further promises in the COBC that it "protect[s] the information about our customers that they entrust to us." Acknowledging that "AT&T possesses sensitive, detailed information about our customers, who rely on AT&T to safeguard that information" and that "[l]aws and regulations tell us how to treat such data," AT&T promises Mr. Terpin, as an AT&T customer, that "[a]ny inappropriate use of confidential customer information violates our customers' trust and may also violate a law or regulation. *Preserving our customers' trust by safeguarding their private data is essential to our reputation.*" (Emphasis added.)

58. Although AT&T acknowledges in its Privacy Policy, as it must, that it could not "guarantee" that Mr. Terpin's "Personal Information will never be disclosed in a manner inconsistent with [AT&T's] Policy (for example, as the result of unauthorized acts by third parties that violate the law or this Policy)," it did not disclose the porosity of its promises to "safeguard[] [customers'] private data." *See* Exh. B at 96. As shown by the events alleged herein, AT&T did not provide even rudimentary protections to protect its own systems from misuse or evasion by its own employees. Indeed, AT&T's employees and individuals working in concert with them were able to avoid what minimal security measures were put in place. Mr. Terpin is not alleging that AT&T failed to have perfect security; rather that it did not even have basic and minimal protections, particularly given its knowledge of the porosity of its current level of protection.

59. As alleged below, AT&T flagrantly and repeatedly violated its commitments to Mr. Terpin in its Privacy Policy and COBC, as well as its legal obligations under the FCA, the CPNI Rules, the Consent Decree, and California law, by willingly turning over to hackers Mr. Terpin's wireless number that allowed hackers to access his "Personal Information" including CPNI. AT&T's betrayal of its obligations caused Mr. Terpin to lose nearly $24 million worth of

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

cryptocurrency. On information and belief, AT&T has also violated its obligations to protect the Personal Information, including CPNI, of numerous other customers who have become victims of SIM theft due to AT&T's negligence and refusal to implement elementary security precautions.

THE PREVALENCE OF SIM CARD SWAP FRAUD

60. AT&T is directly liable for the harm suffered by Mr. Terpin because it has long known that its customers are subject to SIM swap fraud (also called SIM swapping, SIM hijacking, or "port out scam") perpetrated by hackers often with the active cooperation of its own employees and/or agents who readily evade AT&T's ineffectual security measures. SIM swapping (also known as SIM theft or SIM-jacking) consists of the unauthorized insertion of a "SIM" or "Subscriber Identity Module" (also known as a "SIM card") into a mobile device enabling the device to communicate with the service provider. A SIM contains data necessary to make a successful connection between the mobile phone and the telecommunications provider. SIM cards store files that are used to uniquely identify them.

61. A "SIM swap" is a practice whereby a hacker gains access to a victim's telephone account or number by having the carrier install a SIM card for the victim's account into the hacker's phone to redirect communications, including text messages, sent to the victim's mobile telephone on a telephone controlled by the hacker. A perpetrator of a SIM-jack typically arranges through bribery of some person (often an employee of a telecommunications provider) with access to customer information at the carrier to have the carrier change the SIM card assigned to a user to a telephone under the control of the hacker or the hacker's accomplices. Once the SIM transfer has occurred, the hacker uses his or her phone to impersonate the victim with service providers, such as e-mail providers, in order to locate accounts owned by the victim or to request changes to account settings, such as resetting passwords, to take control of the victim's accounts or data.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

62. Perpetrators of SIM swap fraud frequently intercept 2-Factor Authentication (or "2FA") messages sent to the victim's telephone. 2FA is frequently used as a security mechanism for authentication purposes for online accounts, particularly for password changes or for authorization to access an account. Perpetrators of SIM swaps intercept the messages to gain access to the accounts owned by the victim, including cryptocurrency accounts or other accounts that provide access to wallets or accounts. Once the perpetrator gains access to a cryptocurrency wallet or account, the perpetrator transfers the cryptocurrency to wallets or accounts controlled by the perpetrator.

63. The perpetrator of SIM swap fraud and subsequent theft—SIM jackers—specifically target victims who they believe to be investors in cryptocurrency because of the nature of cryptocurrency transactions. The digital assets embodied by cryptocurrency (such as Bitcoin or Ethereum) are a medium of exchange and store of value that uses cryptography to secure the transaction, as well as to store the value. Typically, the holder of cryptocurrency has both a "public" and a "private" key or address that the holder uses to receive, transfer, or use cryptocurrency. The private key, which is individual to the owner of the cryptocurrency, is used to write in the public ledger to transfer cryptocurrency. Because the key can be used to "spend" cryptocurrency, owners typically keep such keys secure. Such keys are complex. For example, in the case of Bitcoin, a 256-bit private key may contain 64 characters consisting of numbers and capitalized and uncapitalized letters.

64. Once a transfer of cryptocurrency has occurred, it cannot be reversed. Cryptocurrency thus makes an attractive target for perpetrators of SIM swap fraud because the perpetrators can transfer stolen digital assets to wallets and/or accounts that are not readily traced or reversed and can be accessed anywhere in the world free from more traditional banking and electronic payments controls.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

65. The nature of SIM swapping has been described in several recent indictments of SIM-jackers. For example, in *United States v. Freeman et al.*, Case No. 2:19-cr-20246 (E.D. Michigan), which is attached hereto as Exhibit E, the indictment described "SIM Hijacking" or "SIM Swapping" as a "tactic [that] enabled The Community [a group of hackers] to gain control of a victim's mobile phone number by linking that number to a subscriber identity module ('SIM') card controlled by The Community—resulting in the victim's phone calls and short message service ('SMS') messages being routed to a device controlled by a member of The Community. Once The Community had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset link be sent via SMS to the device controlled by The Community. Sometimes passwords were compromised by other means, and The Community's device was used to receive two-factor authentication ('2FA') messages sent via SMS intended for the victim." *See* Indictment ¶¶ 3-4.

66. The Indictment in *Freeman* further notes that during SIM swap attacks that hackers "appropriate the online identity of the victim" and that "SIM Hijacking was often facilitated by bribing an employee of a mobile phone provider" or by impersonating the victim. *Id*. ¶¶ 6-8.

67. This description of SIM swapping is echoed in the Criminal Complaint in *United States v. White et al.*, Case No. 2:19-mj-30227 (E.D. Michigan), which was filed on May 2, 2019 and is attached hereto as Exhibit F. In an Affidavit for Probable Cause in *White*, a Special Agent for Homeland Security Investigations, Mark R. Koch, describes SIM swapping in virtual identical terms to that in the *Freeman* case. He further outlines the involvement of Jarratt White and Robert Jack, former contract employees of AT&T in Tucson, in helping to facilitate

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

the thefts of a total of $2,143,471.59 in 41 SIM swaps in the single month of May 2018 for a bribe from the hackers of $4,300.

68. In addition to the foregoing cases, authorities in Santa Clara County have also brought highly publicized felony complaints against three perpetrator of SIM swaps. *See* https://stopsimcrime.org/legal/criminal/california-v-ortizfelony-criminal-complaint/. One of these cases involves Joel Ortiz. As described in a July 30, 2018 *Motherboard* article Ortiz was one of a group of criminals from Boston, who "used the increasingly popular technique known as SIM swapping or SIM hijacking to steal bitcoin, other cryptocurrencies and social media accounts." In a fraud that mirrors the one suffered by Mr. Terpin some months earlier, Ortiz "*specifically targeted people involved in the world of cryptocurrency and blockchain*," including in an incident where he *stole more than $1.5 million from a cryptocurrency entrepreneur who was an AT&T customer*." (Emphasis added)

69. The SIM swapping indictments referenced above have also gained considerable attention from commentators, who have highlighted the culpability of the telecommunications carriers as the weak link. *See, e.g.*, Brian Krebs, "Nine Charged in Alleged SIM Swapping Ring," May 10, 2019: https://krebsonsecurity.com/2019/05/nine-charged-in-alleged-sim-swapping-ring/, "More Alleged SIM Swappers Face Justice," February 6, 2019: https://krebsonsecurity.com/2019/02/more-alleged-sim-swappers-face-justice/; "Alleged SIM Swapper Arrested in California," August 22, 2018 https://krebsonsecurity.com/2018/08/alleged-sim-swapper-arrested-in-california/; "Florida Man Arrested in SIM Swap Conspiracy," August 7, 2018 https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/

70. These reports also confirm the nature of SIM swaps. For example, in an article in *Motherboard* entitled "'Tell Your Dad to Give Us

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Bitcoin:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers," available at https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping the author states that "SIM swapping consists of tricking a provider like AT&T or T-Mobile into transferring the target's phone number to a SIM card controlled by the criminal. Once they get the phone number, fraudsters can leverage it to reset the victims' passwords and break into their online accounts (cryptocurrency accounts are common targets.) In some cases, this works even if the accounts are protected by two-factor authentication. This kind of attack, also known as 'port out scam,' is relatively easy to pull off and has become widespread, as a recent Motherboard investigation showed." Indeed, it is now known that the hack reported in this *Motherboard* article was done by "The Community" with the active involvement of the AT&T employees criminally charged in *United States v. White*.

71. Similarly, the leading security reporter Brian Krebs wrote on August 18, 2018 (https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/) that "SIM swaps are frequently abused by scam artists who trick mobile providers into tying a target's service to a new SIM card and mobile phone that the attackers control. Unauthorized SIM swaps often are perpetrated by fraudsters who have already stolen or phished a target's password, as many banks and online services rely on text messages to send users a one-time code that needs to be entered in addition to a password for online authentication." As Mr. Krebs also wrote: "[i]n some cases, fraudulent SIM swaps succeed thanks to lax authentication procedures at mobile phone stores. *In other instances, mobile store employees work directly with cyber criminals to help conduct unauthorized SIM swaps. . . ."* (Emphasis added.)

72. One of the key common denominators of SIM swap fraud is the temporal proximity between the fact that a victim's phone has been deactivated (once the hackers take over the number) and the loss of cryptocurrency. Typically,

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

the hackers rapidly transfer cryptocurrency out of the victim's wallet or account to wallets and/or accounts under their own control, after which they may "blend" or launder the cryptocurrency to make recovery more difficult if not impossible.

73. As AT&T knows and as these reports and indictments confirm, the prevalence of SIM swapping is facilitated by the active involvement or negligence of AT&T and its employees who faced no restrictions or impediments or either readily overcame or simply bypassed the inadequate security measures that AT&T claims to put in place. This was highlighted by the statements of representatives of the REACT Task Force located in Santa Clara County which has made it its mission to investigate SIM swaps and apprehend hackers. In an interview with Brian Krebs, Caleb Tuttle of REACT stated that SIM swapping happens "in one of three ways. The first is when the attacker bribes or blackmails a mobile store employee into assisting in the crime. The second involves current and/or former store employees who knowingly abuse their access to customer data and the mobile company's network. Finally, crooked store employees may trick unwitting associates at other stores into swapping a target's existing SIM card with a new one." *See* Brian Krebs, "Busting SIM Swappers and SIM Swap Myths," *Krebs on Security*, November 7, 2018, available at https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/ As noted by Mr. Krebs, these attacks are not sophisticated technologically, but are accomplished or aided by coopted AT&T employees who make an end run around the ineffectual protections placed in effect by AT&T.

74. Representatives of the REACT task force directly blamed mobile carriers for the prevalence of SIM swaps stating that "*it's still very, very easy to SIM swap*" and that "*someone needs to light a fire under some folks [at the telecommunications providers] to get these protections in place*." (Emphasis added.) Sgt. Terazi of REACT also noted that "there's a vast disconnect between a mobile company's corporate offices and security policies at the local store level.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

'These are multi-billion companies, and in any big company it's fairly common that the left hand doesn't know what the right hand is doing.'" *Id*.

75. Mr. Terpin alleges on information and belief that AT&T knew well before the attacks on Mr. Terpin that it was subject to widespread SIM swap fraud through the active involvement of its employees. Mr. Terpin further alleges on information and belief that the top echelons of AT&T's parent company, AT&T, Inc., knew of the involvement of AT&T employees in SIM swaps. Based on publicly available information (which is the only information that Mr. Terpin has prior to discovery), Mr. Terpin alleges on information and belief that AT&T's Senior Vice President and Chief Security Officer Bill O'Hern, who has headed AT&T's security operations since 2016 and AT&T's Executive Vice President & Chief Compliance Officer David S. Huntley both had knowledge regarding the structural security flaws and lapses that allowed AT&T employees ready involvement in SIM swapping. *See* https://about.att.com/innovationblog/030116billohern; *see also* https://investors.att.com/corporate-governance/leadership (article on David S. Huntley states that since 2014 he "is responsible for developing policies to safeguard the privacy of customer and employee information, verifying compliance with the legal and regulatory requirements of the countries and jurisdictions where AT&T operates, and ensuring adherence to internal compliance requirements.") In addition, Mr. Terpin alleges that other AT&T officers, including the executives to whom Mr. O'Hern and Mr. Huntley report, were likely to have had knowledge regarding AT&T's failure to implement adequate security protections against SIM swapping.

76. Mr. Terpin alleges further that AT&T knew that cryptocurrency investors like Plaintiff were specifically targeted by SIM swapping through interception of SMS or 2FA messages for password changes and account access and that AT&T was the weak link in such fraud. This is confirmed in

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

numerous articles on SIM swap fraud, including that of Brian Krebs and a July 31, 2018 article in bitcoinist.com entitled "Sim-Swapping Bitcoin Thief Charged in California Court," available at https://bitcoinist.com/sim-swapping-bitcoin-thief-charged-california-court/. The bitcoinist.com article states that "the liability for [SIM swapping] attacks [lies] squarely at the feet of the service providers [which the article calls the 'weakest link'] as security procedures for confirming identity should not be bypass-able using a few pieces of personal information easily obtained online."

77. Mr. Terpin also alleges on information and belief that AT&T's officers, including Chief Compliance Officer David S. Huntley and Chief Security Officer Bill O'Hern because of their job responsibilities for privacy and security knew or should have known that its employees frequently cooperated with hackers and thieves to bypass its security procedures. This is confirmed not only by the reports cited above but also by Brian Krebs, who wrote that "mobile store employees work directly with cyber criminals," and in an August 3, 2018 article in *Motherboard* entitled "How Criminals Recruit Telecom Employees to Help them Hijack SIM Cards," available at https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam, which describes how scammers routinely recruit and pay employees of AT&T and other Telecoms called "plugs" to perform illegal SIM swaps.

78. Mr. Terpin further alleges on information and belief that despite its knowledge that its employees and agents actively cooperate with hackers to rob its own customers, AT&T, including Bill O'Hern and David S. Huntley, is doing nothing to prevent such scams. As an AT&T employee confirmed in the August 3, 2018 *Motherboard* article, "if a criminal finds a corrupt insider, 'there aren't enough safeguards [in place] to stop that employee,' . . .." The AT&T employee further told the author of the article that "*the system is designed so that some*

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

employees have the ability to override security features such as the phone passcode that AT&T (and other companies) now require when porting numbers. 'From there the passcode can be changed,' the employee said in an online chat, referring to a customer information portal that they showed *Motherboard*. 'With a fresh passcode the number can be ported out with no hang ups.'" (Emphasis added.)

79. AT&T officers Bill O'Hern, who is in charge of security, and David S. Huntley, who is in charge of privacy, knew or should have known about the privacy and security flaws that are rampant at AT&T and allowed employees readily to gain access to customer accounts to facilitate SIM swapping.

80. Mr. Terpin alleges on information and belief that countless AT&T customers have been and are continuing to be the victims of SIM swapping and that those customers have lost hundreds of millions of dollars or more because of the fraud. This is confirmed by the indictments that have been brought against hackers and in numerous news stories referenced herein. These indictments literally are the tip of the iceberg of a phenomenon that is plaguing the cryptocurrency community and others, including owners of valuable Instagram and social media accounts.

81. This is further confirmed in the August 18, 2018 article by Brian Krebs, which describes the arrest of Ricky Joseph Handschumacher in Florida, who was charged with grand theft and money laundering for draining cryptocurrency accounts through SIM fraud. According to Krebs, Handschumacher's group came to light "when a Michigan woman called police after she overheard her son talking on the phone and pretending to be an AT&T employee. Officers responding to the report searched the residence and found multiple cell phones and SIM cards, as well as files on the kid's computer that included 'an extensive list of names and phone numbers of people from around the world.'"

82. Krebs' report further revealed that "[t]he Pasco County [Florida] Sheriff's office says their surveillance of the Discord [voice chat] server revealed

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

that the group *routinely paid employees at cellular phone companies to assist in their attacks, and that they even discussed a plan to hack accounts belonging to the CEO of cryptocurrency exchange Gemini Trust Company*." (Emphasis added.)

83. Mr. Terpin alleges on information and belief that AT&T is fully aware of these and numerous other SIM swapping incidents involving its customers, including incidents where its own employees were complicit with hackers. Mr. Terpin further alleges that Bill O'Hern and David S. Huntley and other AT&T executives knew of such incidents because they headed up the security and privacy efforts at AT&T and would thus have been aware of allegations in the press and inquiries of law enforcement authorities. For example, the *Motherboard* article confirms that AT&T had provided investigators with the victim's call records "for the days when the hacker was allegedly in control of the investor's numbers." Indeed, those records were used by law enforcement in issuing a warrant for e-mails from the phone which produced incriminating evidence against Ortiz.

84. Mr. Terpin further alleges on information and belief that federal enforcement agencies have compiled proof that insiders at AT&T cooperated in SIM swap fraud that was directed at members of the cryptocurrency community and that AT&T officers, including Bill O'Hern and David S. Huntley, were aware of the actions and investigations of these law enforcement agencies Mr. Terpin further alleges that such insiders actively cooperated with hackers to provide them customer list information.

85. The prevalence of SIM swap fraud and AT&T's knowledge of such fraud, including the active participation of its own employees in the fraud, demonstrate that the January 7, 2018 SIM swap fraud on Mr. Terpin that led to the theft of nearly $24 million in cryptocurrency was neither an isolated nor an unforeseeable event.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

THE JUNE 11, 2017 HACK

86. On or about June 11, 2017, Mr. Terpin discovered that his AT&T cell phone number had been hacked when his phone suddenly became inoperable. As Mr. Terpin learned from AT&T a few days later, his AT&T password had been changed remotely after 11 attempts in AT&T stores had failed. By obtaining control over Mr. Terpin's phone, the hackers diverted Mr. Terpin's personal information, including telephone calls and text messages, to get access to accounts that use telephone numbers as a means of verification or authentication through the process of 2FA and to change the passwords of those accounts.

87. After the hackers took charge of Mr. Terpin's telephone number, the hackers accessed Mr. Terpin's telephone to divert texts and telephone calls to gain access to Mr. Terpin's cryptocurrency accounts using the SIM swapping method described above. The hackers also used their phone (which now had Mr. Terpin's number) to hijack Mr. Terpin's Skype account to impersonate him. By that means, the hackers convinced a client of Mr. Terpin to send them cryptocurrency and diverted a payment due to Mr. Terpin to themselves. AT&T finally cut off access by the hackers to Mr. Terpin's telephone number on June 11, 2017, but only after the hackers had stolen substantial funds from Mr. Terpin. Moreover, because of the hack, Mr. Terpin expended a substantial amount of time investigating the hack and attempting to repair his computer accounts. As with other SIM swaps, there was a close temporal proximity between Mr. Terpin losing control over his phone and his loss of funds.

88. On or about June 13, 2017, Mr. Terpin met with AT&T representatives in Puerto Rico to discuss the June 11, 2017 hack. Mr. Terpin explained to AT&T that he had been hacked and that the hackers had stolen a substantial amount of money from him. Mr. Terpin expressed concern about AT&T's ineffective security protections and asked how he could protect the

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

security of his phone number and account against future unauthorized access, including hackers attempting to perpetrate SIM swap fraud.

89. In response to Mr. Terpin's request for greater security for his account and in order to induce Mr. Terpin to continue as an AT&T customer, AT&T promised that it would place his account on a "higher security level" with "special protection." AT&T told Mr. Terpin that this "higher security level" would require anyone accessing or changing Mr. Terpin's account to provide a six-digit passcode to AT&T to access or change the account. Anyone requesting AT&T to transfer Mr. Terpin's telephone number to another phone must provide the code. AT&T promised Mr. Terpin at this meeting that the higher security that it was placing on his account, which it also called "high risk" or "celebrity" protection, would ensure that Mr. Terpin's account was much less likely to be subject to SIM swap fraud. AT&T further told Mr. Terpin that the implementation of the increased security measures would prevent Mr. Terpin's number from being moved to another phone without Mr. Terpin's explicit permission, because no one other than Mr. Terpin and his wife would know the secret code. AT&T made all of these promises to convince Mr. Terpin to continue to be an AT&T customer.

90. Mr. Terpin alleges on information and belief that AT&T's "high risk" or "celebrity" protection was created with the knowledge and approval of AT&T's officers, including Bill O'Hern and David S. Huntley, who are in charge of AT&T's security and privacy efforts. Indeed, Mr. Huntley's biography on the AT&T website states that he has direct responsibility for "developing policies to safeguard the privacy of customer . . . information," such as the "high risk" program that AT&T promoted to Mr. Terpin to get him to remain with AT&T after the first SIM swap.

91. At alleged above, AT&T (including Mr. O'Hern and Mr. Huntley) was well aware at the time of the June 11, 2017 incident that its users were subject to SIM swap fraud. It was also well aware that its employees

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

cooperated in such fraud and that the employees could bypass its security procedures. Mr. Terpin alleges on information and belief that AT&T had been previously contacted numerous times by law enforcement authorities about such frauds involving its own employees who actively cooperated with hackers. Given their responsibilities in the company, Mr. O'Hern and Mr. Huntley would have been aware of such contacts and communicated such risks to other executives at AT&T at the highest level. Nonetheless, AT&T recommended that customers who were concerned about fraudulent actions on their account add AT&T's purported "extra security" by adding a "wireless security password" to protect their account. AT&T touted the benefits of such "extra" security on its website because it would require a password for "*managing your account in any retail store.*" *See* https://www.att.com/esupport/article.html#!/wireless/KM1051397 (emphasis added).

92. Mr. Terpin relied upon AT&T's promises that his account would be much more secure against hacking, including SIM swap fraud, after it implemented the increased security measures. Mr. Terpin had no means of knowing that these promises were false and that AT&T, including officers such as Mr. O'Hern and Mr. Huntley, knew that these measures were inadequate because they were being readily bypassed or evaded. Because of AT&T's promises that such measures would be effective, Mr. Terpin retained his account with AT&T. But for these express promises and assurances regarding greater security, Mr. Terpin would have canceled his AT&T account and contracted with a different cellular telephone provider and he would not have lost nearly $24 million from hackers.

93. Mr. Terpin further alleges on information and belief that AT&T, including officers such as Mr. O'Hern and Mr. Huntley, knew at the time that it recommended that he adopt additional security on his account that the additional security measures were not adequate and could be overridden or ignored by its

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

employees. In reality, the vaunted extra protection was, like the Maginot Line, a useless defense that was easily evaded by AT&T's own employees, who it knew or should have known actively cooperated with hackers in SIM swap fraud. Despite AT&T's knowledge of the futility of these actions, AT&T falsely promised Mr. Terpin, to his detriment, that he should implement such additional security measures.

THE JANUARY 7, 2018 SIM SWAP FRAUD

94. AT&T's promises proved to be false and the increased security illusory. On Sunday January 7, 2018, an employee in an AT&T store cooperated with an imposter committing SIM swap fraud. Unbeknownst to Mr. Terpin, AT&T had grossly misrepresented its ability to secure Mr. Terpin's Personal Information after the June 11, 2017 incident. Not only had AT&T failed to disclose that it did not properly supervise, train or monitor its employees to ensure that they scrupulously followed AT&T's security procedures, but it also failed to disclose that it knew that its employees could readily bypass the higher security protection placed on Mr. Terpin's account after the June 11, 2017 hack.

95. On January 7, 2018, Mr. Terpin's phone with his AT&T wireless number went dead. Mr. Terpin was again a victim of SIM swap fraud that allowed a hacker to take control of his phone and to divert 2FA messages to change passwords for and to gain access to Mr. Terpin's accounts and files. As AT&T later admitted, an employee in an AT&T store in Norwich, Connecticut ported over Mr. Terpin's wireless number to an imposter in violation of AT&T's commitments and promises, including the higher security that it had supposedly placed on Mr. Terpin's account after the June 11, 2017 hack that had supposedly been implemented to prevent precisely such fraud. Through the January 7, 2018 hack, thieves gained control over Mr. Terpin's accounts and stole nearly $24 million worth of cryptocurrency from him on January 7 and 8, 2018. There was thus again

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

a close temporal proximity between Mr. Terpin losing control of his phone and the theft of his cryptocurrency.

96. Although the precise method of the theft is known only to the hackers, Mr. Terpin alleges on information and belief that: the hackers used a mobile telephone in their possession with a SIM card with Mr. Terpin's telephone number to identify Mr. Terpin's password protected files or programs; once they had identified such programs, they sent a password reset request to the program or programs which then sent a 2FA message to Mr. Terpin's telephone number, which was by virtue of the SIM swap in the hackers' possession; having gained access to the program or programs with a new password which the hackers constructed, the hackers located a file with confidential information to access Mr. Terpin's wallets and/or accounts holding nearly $24 million of Mr. Terpin's cryptocurrency; and inputting Mr. Terpin's confidential information, they then transferred or attempted to transfer the cryptocurrency to wallets and/or accounts under their control. When he discovered that his cryptocurrency had been transferred, Mr. Terpin requested that exchanges reverse the transactions. It was too late. Virtually all of the cryptocurrency taken by the hackers had been transferred to wallets or accounts exclusively under the hackers' control.

97. When Mr. Terpin's telephone went dead on January 7, 2018, he instantly attempted to contact AT&T to have the telephone number immediately canceled so that the hackers would not gain access to his Personal Information and accounts. Ignoring Mr. Terpin's urgent request, AT&T failed promptly to cancel Mr. Terpin's account, which gave the hackers sufficient time to obtain information about Mr. Terpin's cryptocurrency holdings and to spirit off funds to their own accounts. Adding insult to injury, AT&T placed Mr. Terpin's wife on endless hold (over an hour!) when she asked to be connected to AT&T's fraud department while Mr. Terpin was furiously attempting to see what damage was being done to his accounts. Mr. Terpin's wife never reached AT&T's fraud department because it

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

apparently does not work (or is unavailable) on Sundays. But the hackers work on Sunday!

98. The employees at the AT&T store who unlawfully handed over Mr. Terpin's telephone number to thieves were either blind or complicit. It was impossible to look at Mr. Terpin's account information on the AT&T computer screen and not see the multiple warnings about the need for heightened vigilance, particularly the requirement of a six-digit password. Nonetheless, as AT&T had reason to know before the January 7, 2018 incident (but had never informed Mr. Terpin or other customers), its employees could readily bypass its much-touted security procedures.

99. In cooperating willingly with hackers committing SIM swap fraud to plunder Mr. Terpin's accounts, AT&T violated its own policies as well as the requirements of Section 222 of the FCA and the FCC Consent Decree. On information and belief, AT&T knew that its employees were frequently complicit with SIM swap frauds and could readily bypass its security procedures. Mr. Terpin further alleges that AT&T did not even attempt to require the hacker to provide the six-digit code that AT&T required for access to Mr. Terpin's "high profile" account or to require a supervisor to approve the manual override. Indeed, AT&T admitted to Mr. Terpin on February 4, 2018 that a sales associate in AT&T's Norwich, Connecticut location had violated AT&T's procedures by not only failing to ask for the six-digit code, but also by bypassing its requirement that the hacker have a scannable ID to obtain a replacement SIM card for Mr. Terpin's wireless number. On information and belief, Mr. Terpin alleges that the employee in the AT&T store who handed over the SIM card to the imposter had a criminal record and was cooperating with the hacker and that AT&T had failed properly to supervise the employee, despite its knowledge that its employees cooperated in precisely this type of fraud.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

100. Because of AT&T's cooperation and failure to follow its own policies, the hackers were able to intercept Mr. Terpin's personal information, including telephone calls and text messages, change passwords, access programs and files and locate information that allowed them to gain access to his cryptocurrency wallets and/or accounts.

101. Because of AT&T's willing cooperation with the hacker, gross negligence, violation of its statutory duties, and failure to adhere to its commitments in its Privacy Policy and COBC, as well as its obligations under the FCC Consent Degree and its commitments to Mr. Terpin after the June 11, 2017 hack, Mr. Terpin lost nearly $24 million worth of cryptocurrency.

102. To Mr. Terpin's knowledge, AT&T never informed either the FCC, the FBI or any other law enforcement or regulatory authority about the January 7, 2018 SIM swap. Nor did AT&T ever provide Mr. Terpin with a written explanation of how the SIM swap fraud occurred or a claim form, let alone an apology for facilitating the hack. In contrast, Mr. Terpin himself reported the January 7, 2018 SIM swap to the FBI and the Secret Service Cyber Crimes Unit and has actively sought an investigation of the hack and recovery of the stolen funds.

103. On information, Mr. Terpin alleges that AT&T did not discipline or terminate the employee who turned over a SIM card for his telephone number to imposters and who facilitated the theft of nearly $24 million worth of Mr. Terpin's cryptocurrency.

MR. TERPIN'S SPECIAL RELATIONSHIP WITH AT&T

104. As alleged herein, and to the extent that it is determined to be applicable to certain claims, Mr. Terpin had a "special relationship with AT&T" as defined in *J'Aire Corporation v. Gregory*, 24 Cal. 3d 799, 804 (1979) ("*J'Aire*"). Mr. Terpin undoubtedly had a contract for services with AT&T where he and

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

AT&T were in contractual privity. The services consisted of the provision of mobile telephone services, including the ability not only to make telephone calls, but also to receive messages (including SMS and 2FA communications), access the Internet, send e-mail messages, and access and use a wide variety of programs and applications. *See Riley v. California*, 134 S.Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that happen to have the capacity to be used as a telephone"). AT&T is well aware of the increasingly sophisticated nature of telephone devices, and actively participates in their selling and leasing, and has a variety of plan options for services that are geared toward the ever-expanding uses of such devices.

105. The transaction between AT&T and Mr. Terpin was undoubtedly meant to benefit Mr. Terpin by providing him the ability to use his mobile telephone (or mini-computer) for all of the purposes which he expected and which were intended by AT&T. *See J'Aire*, 24 Cal. 3d at 804.

106. Moreover, it was entirely foreseeable to AT&T that Mr. Terpin would be harmed if he would not longer to be able to use his telephone for its intended purposes and instead that private communications intended for Mr. Terpin were intercepted by hackers. For example, the harm that results from a hacker intercepting a password reset 2FA message is entirely foreseeable in that the hacker changes the password and thus gains control of the program in question (e.g., mail or a file storage site) and can then extract the information in the program for the hacker's own purposes, including accessing cryptocurrency wallets and/or accounts and exfiltrating cryptocurrency to the hacker's own wallets and/or accounts. *Id*.

107. In this case, Mr. Terpin certainly suffered injury by being deprived of almost $24 million in cryptocurrency. *Id*.

108. As required by *J'Aire*, there is also a close connection between AT&T's conduct and the injury suffered by Mr. Terpin. But for AT&T's allowing the hackers to swap Mr. Terpin's SIM into a phone controlled by them, the theft of

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

cryptocurrency could not have happened in close proximity to the swap because the hackers would have had no means of accessing files belonging to Mr. Terpin, resetting his passwords by accessing 2FA message, gaining access to the accounts protected by such passwords, using the information in the accounts to access cryptocurrency wallets and/or accounts, and transferring funds to wallets and/or accounts of their own control. This close connection is further reinforced by the temporal proximity between the SIM swap and the hacks of Mr. Terpin's accounts, as well as the broader general evidence of the increase in SIM swapping and reports of other hacks. *Id*.

109. AT&T's conduct also involves moral blame. Aware of the vulnerability of its customers in having their Personal Information stolen through SIM swapping, AT&T has done nothing to prevent that practice, including enforcing its own privacy policy and adhering to its promises to provide special or additional protection to its customers' accounts. AT&T is also morally culpable in failing to reign in its own employees' knowing or negligent participation in these fraudulent practices. AT&T's behavior is particularly reprehensible regarding Mr. Terpin. AT&T was fully aware that Mr. Terpin had been the victim of SIM jacking and promised that it would put extra protection on his account to retain him as a customer. In fact, AT&T did nothing to protect Mr. Terpin. As one of the world's largest companies, AT&T has the resources to do better and yet it turns an indifferent eye to the widespread violation of the privacy of its own customers. *Id*.

110. Mr. Terpin's lawsuit fulfills the policy of preventing future harm. *J'Aire*. Mr. Terpin's complaint against AT&T has received widespread publicity and has publicized the phenomenon of SIM swapping and the complicity of AT&T in such practice. Because the FCC is apparently not taking an active role in policing AT&T's violations of the FCA, it is up to plaintiffs like Mr. Terpin through lawsuits to help stem AT&T's culpable involvement` in a practice that is leading to widespread harm. This is all the more urgent because AT&T claims to

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

be immune from class actions which would otherwise be a potential vehicle for victims of SIM swaps. *See* AT&T wireless customer agreement discussed in the First Claim for Relief.

FIRST CLAIM FOR RELIEF

(Declaratory Relief: Unenforceability of AT&T Consumer Agreement as Unconscionable and Contrary to Public Policy)

111. Mr. Terpin brings this claim for declaratory relief under 28 U.S.C. § 2201 to have the Court declare that AT&T's wireless customer agreement (the "Agreement") is unconscionable, void against public policy under Cal. Civ. Code §§ 1670.5 and 1668, and unenforceable in its entirety.

112. Mr. Terpin initially entered into a wireless contract with AT&T in or about 2011 when he transferred the account from his wife. Mr. Terpin has asked AT&T for a copy of his agreement, but AT&T refused to provide it to him. Mr. Terpin thus has no copy of any agreement with AT&T for wireless services.

113. The agreement was presented to Mr. Terpin, like all other wireless users, on a take-it-or-leave-it basis. Mr. Terpin had no ability to negotiate any term of the agreement. In contrast, AT&T has virtually unlimited power over its customers, including Mr. Terpin, as seen below by the fact that it purports to hold Mr. Terpin and all other wireless users to the terms of an agreement that they may well have never seen or read.

114. The version of the Agreement posted in early 2018 purports to govern AT&T's provision of wireless service to all customers, including Mr. Terpin who first contracted with AT&T over two decades ago. A true and correct copy of the Agreement posted on AT&T's website in early 2018 at https://www.att.com/legal/terms.wirelessCustomerAgreement-list.html is attached hereto as Exhibit D. As alleged below, the Agreement contains numerous unconscionable terms that renders it unenforceable in its entirety because its

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

"central purpose . . . is tainted with illegality." *Ingle v. Circuit City Stores, Inc.*, 328 F.3d 1165, 1180 (9th Cir. 2003) (holding invalid an agreement that obstructs the ability of customers to bring any claims against defendant).

115. The Agreement states that the Agreement and other agreements that are "not otherwise described below that are posted on applicable AT&T websites or devices, and any documents expressly referred to herein or therein, make up the complete agreement between you and AT&T and supersede any and all prior agreements and understandings relating to the subject matter of this Agreement." Through such vague language, AT&T apparently contends that not only the Agreement, but other unspecified and unknown agreements, bind all wireless customers, whether or not such customers have seen the Agreement or are aware of its terms. In other words, every time AT&T mints a new (and more onerous) version of its agreements, its unsuspecting customers are purportedly bound by the new terms. This practice highlights the fact that not only are these contracts not negotiable, they are invisible. What you don't see, you still get.

116. The Agreement is a classic contract of adhesion imposed by AT&T upon a party with no bargaining power. In contrast, AT&T has unchecked power to insist upon its own terms even if the consumer is unaware of the terms of the Agreement itself. There is no ability to negotiate any term of the Agreement. It is literally "take it or leave it."

117. The Agreement is void as against public policy under Cal. Civ. Code § 1668 as a contract of adhesion purporting to bind customers who have never heard or seen the agreement and most likely are entirely unaware of its provisions. The Agreement is void and unenforceable in its entirety because it also contains exculpatory provisions, damage waivers, and an indemnification provision that purport to prevent consumers from bringing *any* claims against AT&T or obtaining redress for their claims -- even for billing errors.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

118. The exculpatory provision in Paragraph 4.1 of the Agreement ("Exculpatory Provision") contains numerous provisions that are contrary to public policy under Cal. Civ. Code § 1668 because they attempt to exempt AT&T from responsibility for its own gross negligence, fraud, and violations of law. In pertinent part, the Exculpatory Provision states that:

> ***WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE OR COVERAGE.*** . . . AT&T MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY, ***SECURITY OR PERFORMANCE REGARDING ANY SERVICES, SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE***, for any:
>
> a. act or omission of a third party;
>
> b. mistakes, omissions, interruptions, errors, failures to transmit, delays, or defects in the Services or Software provided by or through us;
>
> c. ***damages or injury caused by the use of Services, Software, or Device***, including use in a vehicle . . ..

(Capitalization in original; emphasis added in bold and italics.)

119. The Exculpatory Provision renders the entire Agreement unenforceable on public policy grounds under Cal. Civil Code §§ 1668 and 1670.5 because it purports to exempt AT&T from its gross negligence, statutory violations and willful behavior, including the egregious conduct alleged herein. The Exculpatory Provision is further against public policy because it purports to exempt AT&T from violation of statutory obligations, including the obligation to maintain the confidentiality and security of its customers' private and personal information under Section 222 of the FCA, the FCC Consent Degree, and numerous provisions

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

of California State law, including California unfair competition law, the Consumer Legal Remedies Act, and the California Customer Records Act. Thus, even where, as here, AT&T willfully violates its statutory duties under the FCA and the Consent Decree, not to mention its promises in its Privacy Policy and the COBC, a customer is prevented by the Exculpatory Provision from bringing a claim for negligent or willful disclosure of the customer's Personal Information, including CPNI, because such claim seeks redress for "damages or injury caused by the use of Services, Software, or Device . . ." and is waived by the Exculpatory Provision.

120. AT&T also seeks in the contract to have customers waive any damages, except for providing a "credit equal to a pro-rata adjustment of the monthly Services fee for the time period your Services was unavailable, not to exceed the monthly Service fee" when a customer's services are interrupted.

121. Section 4.1 of the Agreement ("Damages Restriction") is also void under Cal. Civ. Code §§ 1668 and 1670.5 because it purports to exempt AT&T for all other damages:

> Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries.

122. The Exculpatory Provision is invalid under Civil Code § 1670.5 because it allocates all the risks to the consumer with AT&T disclaiming any damages for its own conduct—even fraud, gross negligence, and statutory violations, including those governed by the FCA. Thus, even if AT&T deliberately handed over a customer's CPNI to hackers in violation of Section 222 of the FCA, a customer would not be entitled to the full range of damages afforded by that statute under the Damages Restriction.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

123. The Damages Restriction included in a contract of adhesion as to which AT&T's users, including Mr. Terpin, have no bargaining authority, is void because it is plainly unconscionable and against public policy. The Damages Restriction is contained in a lengthy form contract drafted by a domineering telecommunication provider with vast assets in a far superior bargaining position to the wireless user. Indeed, it is no exaggeration to say that the consumer has no bargaining power as regards AT&T, particularly as to the Damages Restriction and other draconian provisions in the Agreement. Because the Damages Restriction is found in a document posted on a website that, by fiat, is automatically made applicable to customers, customers may not even be aware that they have virtually no redress against AT&T, unless they diligently monitor changes in the website. Moreover, the Damages Restriction is contained in a complex and lengthy contract that provides essential wireless services—without which most customers have no means of communication (including for emergency services), let alone essential computing, geolocation, texting, research or other services.

124. The Damages Restriction is also substantively unconscionable because it allocates risks in an objectively unreasonable manner. *See Armendariz v. Foundation Health Psychcare Services, Inc.*, 24 Cal. 4th 83, 113-114 (2000). The allocation of risks under the Agreement is objectively unreasonable because AT&T—a telecommunications behemoth with billions of dollars of assets and tens of millions of customers—takes upon itself virtually no liability (other than minimal recompense for interrupted services) and purports to exempt itself from virtually all damages, including those arising out of its own deliberate, grossly negligent, or fraudulent acts.

125. The Agreement is further unenforceable because customers are purportedly required to indemnify AT&T for all claims arising out of the services provided by AT&T, including claims that arise due to AT&T's negligence, gross

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

negligence, deliberate conduct, or statutory violations. The indemnity provision in Paragraph 4.1 of the Agreement ("Indemnity") states:

> To the full extent allowed by law, you hereby release, indemnify, and hold AT&T and its officers, directors, employees and agents harmless from and against *any and all claims of any person or entity for damages of any nature arising in any way from or relating to, directly or indirectly, service provided by AT&T* or any person's use thereof (including, but not limited to vehicular damage and personal injury), *INCLUDING CLAIMS ARISING IN WHOLE OR IN PART FROM THE ALLEGED NEGLIGENCE OF AT&T,* or any violation by you of this Agreement.

(Capitalization in original; emphasis added.)

126. Read literally, the Indemnity requires a consumer, such as Mr. Terpin, to hold AT&T harmless for AT&T's own negligence, deliberate behavior, gross negligence, statutory violations (including disclosure of CPNI under the FCA), or fraud if the conduct is related "directly or indirectly" to any "service provided by AT&T." On its face, the indemnity provision in a contract of adhesion renders the entire Agreement unconscionable and unenforceable because if defeats the entire purpose of the contract by making it impossible for consumers to bring claims against AT&T for the entire range of statutory rights to which a consumer, such as Mr. Terpin, is entitled. Indeed, the Indemnity would totally obviate AT&T's commitment to privacy in its Privacy Policy as well as its legal obligations under the FCA, the CPNI Rules, and the Consent Decree.

127. Because the entire Agreement is unenforceable because the central purpose of the Agreement is "tainted with illegality . . . [so that] the contract as a whole cannot be enforced," the arbitration provision in Paragraph 2.2 of the Agreement ("Arbitration Provision") is also unenforceable. *See*, *Armendariz*, 24 Cal. 4th at 89-90.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

128. The Arbitration Provision would require Mr. Terpin to arbitrate his claims "without affording the full range of statutory remedies, including punitive damages and attorney fees" that are available to him under the claims alleged herein. *Armendariz*, 24 Cal. 4th at 103 (damages limitation unlawful if applied to statutory claims). For example, Mr. Terpin, if required to arbitrate this claim, would be forced by the Damages Limitation to forego his entitlement to punitive damages for AT&T's fraud and negligence. Moreover, the Arbitration Provision would require Mr. Terpin to forego the full range of damages to which he is entitled under his Second Claim for Relief under the Federal Communications Act § 222. These defects render not only the Arbitration Provision, but also the entire Agreement, unenforceable.

129. Because the defenses raised by Mr. Terpin as to the unconscionability of the Agreement are "enforced evenhandedly" and do not "interfere[] with the fundamental attributes of arbitration," they do not run afoul of *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court's decision in *Concepcion* did not abrogate the savings clause of the FAA that provides that arbitration agreements may be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract," including "generally applicable contract defenses, such as fraud, duress, or unconscionability." *Concepcion* at 339, *quoting* 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*, 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses apply squarely to the Agreement.

130. There is an actionable and justiciable controversy between Mr. Terpin and AT&T in that Mr. Terpin contends that the Agreement, including the Exculpatory Provision, Damages Restriction, Indemnity and Arbitration Provision, is unenforceable in its entirety because it is unconscionable and void against public policy since it prevents consumers, such as Mr. Terpin, from obtaining redress

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

against AT&T even for deliberate acts in violation of its legal duties. AT&T undoubtedly disagrees.

131. A judicial declaration of the enforceability of the Agreement, including the Exculpatory Provision, Damages Restriction, Indemnity and Arbitration Provision and all other provisions of the Agreement, is necessary and appropriate.

132. Mr. Terpin seeks a judgment declaring that the Agreement in its entirety is unenforceable as unconscionable and against public or, in the alternative that (a) the Exculpatory Provision is unenforceable as against Mr. Terpin; (b) the Damages Restriction is unenforceable against Mr. Terpin; (c) the Indemnity is unenforceable as against Mr. Terpin; and (d) the Arbitration Provision is unenforceable as against Mr. Terpin

SECOND CLAIM FOR RELIEF

(Unauthorized Disclosure of Customer Confidential Proprietary Information and Proprietary Network Information

(Federal Communications Act, 47 U.S.C. §§ 206, 222))

133. Plaintiff realleges the allegations in Paragraphs 1-132 as if fully set forth herein.

134. AT&T is a "common carrier" engaging in interstate commerce by wire regulated by the Federal Communications Act ("FCA") and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

135. Under section 206 of the FCA, 47 U.S.C. § 206, "[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case."

136. Section 222(a) of the FCA, 47 U.S.C. § 222(a), requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers ("CPI").

137. Section 222(c)(1) of the FCA, 27 U.S.C. § 222(c)(1) further requires that, "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information ['CPNI'] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services. . .."

138. The information disclosed to hackers by AT&T in the January 7, 2018 SIM swap fraud transferring Mr. Terpin's telephone number, was CPI and CPNI under Section 222 of the FCA.

139. AT&T failed to protect the confidentiality of Mr. Terpin's CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers in the January 7, 2018 SIM swap fraud. Through its negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the terms of the Consent Decree, the warnings of the Pretexting Order, its Privacy Policy and the COBC, and by allowing its employees to bypass such procedures, AT&T permitted hackers to access Mr. Terpin's telephone number, telephone calls, and text messages, which gave them access to 2FA messages, which they used to reset the passwords on Mr. Terpin's accounts by use of one or more 2FA messages to gain access to files on those accounts that contained the confidential information necessary to access Mr.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Terpin's wallets. Once they had access to the wallets, they transferred the cryptocurrency into wallets and/or accounts under their control which resulted in a loss to Mr. Terpin of nearly $24,000,000 worth of his cryptocurrency.

140. As a direct consequence of AT&T's violations of the FCA, Mr. Terpin has been damaged by loss of nearly $24,000,000 worth in cryptocurrency which AT&T allowed to fall into the hands of thieves, and for other damages in an amount to be proven at trial. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 59-82, and 91-92.

141. Mr. Terpin is also entitled to his attorney's fees under the FCA in bringing this action against AT&T for its gross negligence and fraudulent misrepresentation as to the security that it provides for customer accounts as required by the FCA, the CPNI Regulation, and the Consent Decree.

THIRD CLAIM FOR RELIEF

(Deceit by Concealment—Cal. Civ. Code §§ 1709, 1710)

142. Mr. Terpin realleges the allegations of Paragraphs 1-141 as if fully set forth herein.

143. As alleged above, AT&T, including Chief Security Officer Bill O'Hern and Chief Compliance Officer David S. Huntley, who are respectively in charge of AT&T's security and privacy protections, knew that its data security measures were grossly inadequate, that its employees and agents could readily bypass the procedures, that its employees actively cooperated with hackers and thieves, and that it was incapable of living up to its commitments to consumers, including to Mr. Terpin, under state and federal law, as well as under its own Privacy Policy, to protect his Personal Information, including CPI and CPNI. Nonetheless, to induce Mr. Terpin to remain as an AT&T customer after the June 11, 2017 hack, AT&T promised Mr. Terpin that it would implement AT&T's additional levels of security requiring a six-digit passcode to make modifications to

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

his account. Because of their responsibilities at AT&T, Mr. O'Hern and Mr. Huntley were aware of this program and of its inadequacies. In contrast, Mr. Terpin took what he was told about this AT&T program at face value and was unaware that AT&T's security measures were not state of the art. In contrast to other carriers, such as T-Mobile, AT&T did not provide a SIM lockdown with its higher level of security.

144. To reiterate, Mr. Terpin alleges on information and belief that AT&T, authorized by Mr. O'Hern and Mr. Huntley, made the following specific concealments of material facts: (1) In June 2017, after the initial SIM swap, AT&T representatives encouraged Mr. Terpin to adopt additional security measures (adding a six digit code) without telling Mr. Terpin that such security measures could readily be evaded or bypassed by AT&T employees acting in concert with individuals perpetrating SIM swap fraud; (2) at all times herein relevant prior to the second SIM swap in January 2018, AT&T concealed the fact that its employees frequently acted in concert with individuals perpetrating SIM swap fraud to provide such individuals with personal information about its mobile users; (3) at all times herein relevant prior to the second SIM swap in January 2018, AT&T concealed the fact that its employees frequently acted in concert with individuals perpetrating SIM swap fraud to provide such individuals with direct access to their customers' accounts, which enabled such individuals to intercept 2FA messages to customers; and (4) because of the inadequacies of AT&T's security measures and the active participation of its employees in SIM swaps that AT&T's promises in its Privacy Policy had no value.

145. As further alleged above, AT&T, including Mr. O'Hern and Mr. Huntley, knew or should have known from prior incidents and contacts with law enforcement that its system was subject to SIM swap fraud, that its employees cooperated with hackers in such fraud, that such fraud was prevalent in the cryptocurrency community, and that its security measures were ineffective in

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

preventing the fraud. Mr. O'Hern should have been well aware of this because he is in charge of security and AT&T and Mr. Huntley should have known because he is in charge of insuring that AT&T protects the privacy of its customers.

146. In response to these facts, AT&T chose to do nothing to protect Mr. Terpin and instead made false promises to him to induce him to remain as an AT&T customer.

147. Although AT&T stated in the Privacy Policy that it could not "guarantee" that customers' "Personal Information will never be disclosed in a manner inconsistent with [AT&T's] Policy . . ," it knew that its low level employees and contractors could readily sidestep AT&T security protections or that such protections were non-existent. Such employees were also susceptible to relatively small bribes from SIM swappers. Although Mr. Terpin understands that no security measure is perfect, he reasonably relied on AT&T's promises in the privacy policy that it would protect his personal information against obvious and easily avoidable security flaws. Mr. Terpin's expectations were reasonable given AT&T's vast resources. Mr. Terpin is not alleging that AT&T erred by not having perfect security, but by not having any security worth the name.

148. AT&T representatives also specifically promised Mr. Terpin additional protection after the initial June 2017 SIM swap. Mr. Terpin accepted their promises at face value. Mr. Terpin had no reason to doubt that these security measures would be effective and had no knowledge at that time that an AT&T employee had been involved in his initial SIM swap.

149. At all times, including at the time it promised Mr. Terpin additional security after his initial June 2017 SIM swap, AT&T had an obligation to disclose to Mr. Terpin that his Personal Information, including CPI and CPNI, was readily obtained by hackers and that its own employees handed such information to hackers, and yet did not implement measures to protect Mr. Terpin or willfully failed to adhere to any measures that were in place, including its so-called "higher

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

security level" for high profile or celebrity accounts and its required security and training measures under the Consent Decree. AT&T's promises of security, which come from officers such as Bill O'Hern and David S. Huntley, who are in charge of security and privacy at the company, were false and it knew at the time it made such promises that they were ineffective and could be readily overridden by its employees. As AT&T's officers knew, AT&T's so-called security system more resembles a thin slice of swiss cheese than a sophisticated network of "heightened security."

150. AT&T did not disclose these things to Mr. Terpin and willfully deceived Mr. Terpin by concealing the true facts concerning its data security, which AT&T was legally obligated and had a duty to disclose. It did so in order to induce Mr. Terpin to remain as its customer. It is far easier to penetrate AT&T's system than obtaining a new password from Walmart.

151. Had AT&T disclosed the true facts about its dangerously poor data security practices, its inadequate supervision and training of its employees, and the fact that its employees can readily bypass the additional security measures that it encouraged Mr. Terpin to place on his account, Mr. Terpin would have taken further measures to protect himself and would have ceased being a customer of AT&T. Mr. Terpin justifiably relied on AT&T's statements, including statements after the June 11, 2017 hack regarding the effectiveness of the additional security it encouraged for his account, and further relied on AT&T to provide accurate and complete information about its data security in continuing to be AT&T's customer.

152. Rather than disclosing the inadequacies in its security, including the additional security it encouraged Mr. Terpin to place on his account, AT&T willfully suppressed any information relating to such inadequacies.

153. AT&T's actions are "deceit" under Cal. Civ. Code § 1710 in that they are the suppression of a fact by one who is bound to disclose it, or who

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

gives information of other facts which are likely to mislead for want of communication of that fact.

154. Because of the deceit by AT&T, it is liable under Cal. Civ. Code § 1709 for "any damage which [Mr. Terpin] thereby suffers."

155. Because of this deceit by Defendants, Mr. Terpin's Personal Information, including his CPI and CPNI, as described above, *inter alia*, in Paragraphs 91-92 was compromised by hackers and he was deprived of nearly $24 million worth of cryptocurrency. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 59-82, and 91-92. In addition, Mr. Terpin's Personal Information is now easily available to hackers, including through the Dark Web. Mr. Terpin is further damaged to the extent of the amounts that he has paid AT&T for wireless services, because those services were either worth nothing or worth less than was paid for them because of lack of security. Mr. Terpin has also suffered substantial out-of-pocket costs because of AT&T's inadequate security.

156. Because AT&T's deceit is fraud under Civil Code § 3294(c)(3), and AT&T's conduct was done with malice, fraud and oppression, Mr. Terpin is entitled to punitive damages under Civil Code § 3294(a). Mr. Terpin further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

FOURTH CLAIM FOR RELIEF

(Misrepresentation)

157. Mr. Terpin realleges Paragraphs 1 through 156 as if fully set forth herein.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

158. As alleged herein, *inter alia*, in Paragraphs 104-110, and to the extent determined to be applicable to this claim, Mr. Terpin and AT&T have a special relationship as such term is used in *J'Aire*.

159. AT&T made numerous representations and false promises in its Privacy Policy and COBC as well as in its advertising, that it would maintain the security of its customers' personal information, including Mr. Terpin's Personal Information. Separate from the documents, an AT&T employee made specific promises to Mr. Terpin after the June 11, 2017 hack regarding the security protection that would be given to Mr. Terpin's personal information by adding a six-digit security code on the account. The AT&T employee did so in order to persuade Mr. Terpin not to cancel his AT&T service.

160. AT&T did not intend to perform either its promises in the Privacy Policy or after the June 11, 2017 hack because it knew that its security protections, including the six-digit security code, were ineffectual and could easily be evaded or bypassed by its employees. Such representations and promises were also false because AT&T was using outdated security procedures and failed to disclose that it did not adhere to its own standards, including the heightened security standards that it implemented for Mr. Terpin after the June 11, 2017 hack, the CPNI Rules or the procedures mandated by the Consent Decree. AT&T further knew that it did not have in place state-of-the-art security protections, such as a SIM lock out. Mr. Terpin further alleges on information and belief that AT&T decided not to implement technological measures to prevent SIM swapping because it did not want to expend the money for such measures and did not wish to hamper the lucrative practice of having mobile users swap or upgrade their devices.

161. AT&T's misrepresentations and false promises, including those made after the June 11, 2017 hack, were material to Mr. Terpin who reasonably relied upon the representations and promises. Specifically, Mr. Terpin relied on AT&T's false promise regarding the effectiveness of the additional six-digit code

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

protection on his account to continue as an AT&T customer. Mr. Terpin would not have agreed to continue to use and pay for AT&T's services if he had known that the additional security protection was ineffective and that AT&T's other security measures were not as secure as represented by AT&T and would not have lost nearly $24 million.

162. AT&T intended that Mr. Terpin rely on their representations and promises, including those made after the June 11, 2017 hack, as it knew that Mr. Terpin would not entrust his Personal Information to unreasonable security risks, particularly because Mr. Terpin had been subject to the June 11, 2017 hack. In reliance upon AT&T's representations and promises, Mr. Terpin continued to maintain a wireless account with AT&T and to use his AT&T phone number for verification and other purposes.

163. As a direct and proximate result of AT&T's wrongful actions, Mr. Terpin has been damaged by paying monthly fees to AT&T and having thieves steal nearly $24 million worth of cryptocurrency through the January 7, 2018 SIM swap fraud. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 59-82, and 91-92.

164. AT&T's misconduct is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T conducted with the intent on the part of AT&T of depriving Mr. Terpin of legal rights or otherwise causing injury. AT&T's conduct was done with malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) and Mr. Terpin is entitled to punitive damages against AT&T under Civil Code §3294(a).

165. Mr. Terpin further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

FIFTH CLAIM FOR RELIEF

(Negligence)

166. Plaintiff realleges the allegations in Paragraphs 1 through 165 as if fully set forth herein.

167. As alleged herein, *inter alia*, in Paragraphs 104=110, and to the extent determined to be applicable to this claim, AT&T and Mr. Terpin had a special relationship as such term is used in *J'Aire*.

168. AT&T owed a duty to Mr. Terpin to exercise reasonable care in safeguarding and protecting his Personal Information, including CPI and CPNI, and keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Mr. Terpin's Personal Information, including CPI and CPNI, was adequately secured and protected. AT&T had a further duty to implement and adhere to the "high security" or "celebrity" protocol that it had promised Mr. Terpin that it would place on his account to protect his Personal Information and had a duty to adhere to the FCA, CPNI Rules, and the provisions of the Consent Decree.

169. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. Indeed, AT&T acknowledged this in its Privacy Policy and in agreeing, at Mr. Terpin's request, to place additional "high security" measures on Mr. Terpin's account to prevent hackers from committing SIM swap fraud on Mr. Terpin. AT&T further promoted its "extra security" on its website. AT&T likewise knew that Mr. Terpin's Personal Information was vulnerable to hacks by thieves and other criminals both because it

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

acknowledged such in its Privacy Policy and because it had been informed by Mr. Terpin of the June 11, 2017 hack. AT&T thus knew of the substantial harms that could occur to Mr. Terpin if it did not place adequate security on his Personal Information and did not follow its own "high security" measures for the account.

170. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T would take appropriate measures to protect it. But AT&T did not protect Mr. Terpin's Personal Information and violated his trust. AT&T knew its security was inadequate in part due to the FCC investigation that led to the Consent Decree. AT&T is morally culpable, given prior security breaches involving its own employees.

171. AT&T breached its duty to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, CPNI Rules, the Consent Decree, and its own Privacy Policy.

172. AT&T's failure to comply with federal and state requirements for security further evidences AT&T's negligence in failing to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI.

173. But for AT&T's wrongful and negligent breach of its duties owed to Mr. Terpin, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency. The

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 59-82, and 91-92.

174. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including his CPI and CPNI. The harm was additionally foreseeable in that AT&T was aware that Mr. Terpin was a holder and user of cryptocurrency and a potential victim of hacking following the June 11, 2017 hack.

175. AT&T's misconduct as alleged herein is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

176. Mr. Terpin further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

SIXTH CLAIM FOR RELIEF

(Negligent Supervision and Training)

177. Mr. Terpin realleges the allegations of Paragraphs 1 through 176 as if fully set forth herein.

178. As alleged herein, *inter alia*, in Paragraphs 104-110, and to the extent determined to be applicable to this claim, AT&T and Mr. Terpin had a special relationship as such term is used in *J'Aire*.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

179. AT&T owed a duty to Mr. Terpin to exercise reasonable care in supervising and training its employees to safeguard and protect his Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty included AT&T's instructing its employees to adhere to the "high security" or "extra security" protocols that AT&T had promised Mr. Terpin it would place on his account to protect his Personal Information.

180. AT&T was aware of the ability of its employees to bypass its security measures and the fact that its employees actively participated in fraud involving its customers, including pretexting and SIM card swap fraud, by bypassing such security measures.

181. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr. Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by thieves and other criminals because it had been informed by Mr. Terpin of the June 11, 2017 hack.

182. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T's employees would take appropriate measures to protect it. AT&T also made promises in the COBC that its employees would respect its customers' privacy and was further required by the Consent Decree to supervise and train its employees to adhere to its legal obligations to protect their Personal Information.

183. AT&T breached its duty to supervise and train its employees to safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI, by not requiring them to adhere to its obligations under the CPNI Rules, the Consent Decree and other legal provisions. On January 7, 2018, AT&T's

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

employees facilitated SIM swap fraud on Mr. Terpin by not requiring individuals requesting Mr. Terpin's telephone number to present valid identification. AT&T employees also failed to follow AT&T's "higher" or "extra" security by not requiring the individual requesting Mr. Terpin's telephone number to provide the secret six-digit code that AT&T had given Mr. Terpin to prevent precisely such fraud.

184. AT&T knew its supervision and monitoring of its employees was inadequate through: a) the FCC investigation that led to the Consent Decree mandating measures to improve such training and monitoring; and b) its knowledge from prior incidents that its employees cooperated with hackers in SIM swap fraud. AT&T is morally culpable, given prior security breaches involving its own employees.

185. AT&T breached its duty to exercise reasonable care in supervising and monitoring its employees to protect Mr. Terpin's Personal Information, including CPI and CPNI.

186. AT&T's failure to comply with the Consent Decree and to follow the requirements of the FCA and CPNI Rules further evidence AT&T's negligence in adequately supervising and monitoring its employees so that they would safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI.

187. But for AT&T's wrongful and negligent breach of its duties to supervise and monitor its employees, Mr. Terpin's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 59-82, and 91-92. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency.

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

188. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to supervise and monitor its employees in safeguarding and protecting Mr. Terpin's Personal Information, including his CPI and CPNI.

189. AT&T's misconduct as alleged here is done with malice, fraud and oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

190. Mr. Terpin further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

SEVENTH CLAIM FOR RELIEF

(Negligent Hiring)

191. Mr. Terpin realleges the allegations in Paragraphs 1 through 190 as if fully set forth herein.

192. As alleged herein, *inter alia*, in Paragraphs 104-110, and to the extent determined to be applicable to this claim, AT&T and Mr. Terpin had a special relationship as such term is used in *J'Aire*.

193. AT&T owed a duty to Mr. Terpin to exercise reasonable care in hiring competent, honest, and ethical employees to safeguard and protect his Personal Information, including CPI and CPNI, to keep it from being compromised, lost, stole, misused and/or disclosed to unauthorized parties. AT&T also owed a

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

duty to exercise reasonable care in the operation of AT&T stores, including by third parties, and their hiring of employees for those AT&T stores.

194. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr. Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by thieves and other criminals because it had been informed by Mr. Terpin of the June 11, 2017 hack. AT&T further knew from the investigation that led to the Consent Decree that its employees had cooperated with hackers and thieves by turning over to them the CPNI of its customers to facilitate fraud and theft. It also knew from prior incidents of SIM swap fraud that its employees cooperated with hackers and thieves defrauding AT&T's own customers.

195. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T's employees would take appropriate measures to protect it. AT&T also made promises in the COBC that its employees would adhere to AT&T's ethical and legal obligations, including respecting its customers' privacy. AT&T was further required by the Consent Decree to correct the practices that had led to hiring employees who had cooperated with hackers and thieves and stolen customers' personal information.

196. AT&T breached its duty to hire employees who would safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI. Mr. Terpin alleges on information and belief, that the employees who facilitated the SIM swap fraud perpetrated on Mr. Terpin did not live up to AT&T's purported ethical standards, as expressed in the COBC, or to their legal obligations to Mr. Terpin. Mr. Terpin further alleges on information and belief, that the employee at the AT&T store who ported Mr. Terpin's telephone number to the hackers on

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

January 7, 2018, had a criminal record and colluded with the hackers in perpetrating the fraud on Mr. Terpin.

197. AT&T knew that its hiring of employees was inadequate through the FCC investigation that led to the Consent Decree that revealed that employees had actively handed over the Personal Information of its customers to hackers and thieves. AT&T is morally culpable, given the prior conduct of its employees.

198. AT&T breached its duty to properly hire competent, honest and ethical employees to protect Mr. Terpin's Personal Information, including CPI and CPNI.

199. AT&T's failure to comply with the Consent Decree is further evidence of its failure to investigate employees to ensure that they adhered to AT&T's ethical and legal responsibilities.

200. On information and belief, the employee or agent at the AT&T store who gave Mr. Terpin's SIM card to the imposter on January 7, 2018 was Jahmil Smith. Smith has a criminal record which AT&T should have discovered before or after hiring him.

201. But for AT&T's wrongful and negligent breach of its duties to hire ethical and competent employees, Mr. Terpin's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM swap fraud. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 60-85, and 95-96. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly $24 million worth of cryptocurrency.

202. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to hire competent and ethical employees who would safeguard and protect Mr. Terpin's Personal Information, including his CPI

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

and CPNI. Indeed, this failure on the part of AT&T led to the January 7, 2018 SIM swap fraud.

203. AT&T's misconduct as alleged herein is malice, fraud and oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

204. Mr. Terpin further alleges on information and belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had advance knowledge of the inadequacies of AT&T's security, the participation of AT&T employees in evading or bypassing security, and they committed or ratified the acts of oppression, fraud or malice alleged herein.

EIGHTH CLAIM FOR RELIEF

(Breach of Contract – Privacy Policy)

205. Mr. Terpin realleges the allegations in Paragraphs 1 through 204 as if fully set forth herein.

206. The Privacy Policy is a binding contract between AT&T and Mr. Terpin.

207. AT&T breached the contract with respect to at least the following provisions of the Privacy Policy:

- AT&T's promise that it will not sell or disclose users' "Personal Information" to anyone;
- AT&T's commitments that it has "worked hard to protect your information" and has "established electronic and administrative safeguards designed to make the information we collect secure";

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

- AT&T's promise that its employees must follow its COBC and that "all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records";
- AT&T's promise that it subjects employees who do not meet its security standards to "disciplinary action" and dismissal;
- AT&T's promise that it has "implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information";
- AT&Ts promise that it "maintain[s] and protect[s] the security of computer storage and network equipment";
- AT&T commitment that it limits access to Personal Information "to only those with jobs requiring such access"; and
- AT&T's promise that it "[r]equire[s] caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information."

208. AT&T also breached its COBC by failing to follow "not only the letter of the law, but the spirit of the law" and failing to "protect the privacy of our customers' communications because "not only do our customers demand this, but the law requires it."

209. AT&T breached these provisions of its Privacy Policy and COBC by not having proper safeguards in accordance with law, including the FCA, CPNI Rules, and the Consent Decree, and Cal. Civ. Code §1798.81.5, to protect

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Mr. Terpin's "Personal Information," including CPI and CPNI. AT&T further breached its promises by not limiting access to Mr. Terpin's Personal Information to authorized or properly trained individuals. AT&T likewise violated its commitments to maintain the confidentiality and security of Mr. Terpin's Personal Information by failing to comply with its own policies and applicable "law, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records." AT&T thus breached its obligations under the FCA, CPNI Rules, the Consent Decree and California law.

210. The January 7, 2018 SIM swap fraud was a direct and legal cause of the injuries and damages suffered by Mr. Terpin, including loss of nearly $24 million of crypto currency.

211. To the extent that AT&T maintains that the Exculpatory Provision, Damages Restriction, and the Indemnity in the Agreement apply to the promises made by AT&T in the Privacy Policy and the COBC, such provisions, as well as the Agreement in its entirety, are unenforceable and do not apply to the Privacy Policy and COBC. *See* Cal. Civ. Code §§1670.5, 1668 (contracts are unenforceable if unconscionable or void against public policy); *Ingle v. Circuit City Stores, Inc.*, 328 F.3d 1165, 1180 (9th Cir. 2003) (contracts void if central purpose is tainted with illegality). Moreover, such provisions are unconscionable under California law because an entity cannot exculpate itself from its obligations to maintain the privacy and security of personal information under federal and California law, as further set forth herein in Paragraphs 70 to 82. *See Health Net of California, Inc. v. Department of Health Services*, 113 Cal. App. 4th 224, 244 (2004) (California courts for 85 years have invalidated "contract clauses that relieve a party from responsibility for future statutory and regulatory violations")

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

Mr. Terpin was harmed due to AT&T's breach of the terms of the Privacy Policy and COBC, because his "Personal Information," including CPI and CPNI, was breached in the January 7, 2018 SIM swap fraud, which led to monetary losses of nearly $24 million. The connection between AT&T, the SIM swap and the loss of Mr. Terpin's cryptocurrency is alleged herein, *inter alia*, in Paragraphs 12-13, 60-85 and 95-96.

PRAYER FOR RELIEF

Wherefore, Plaintiff Michael Terpin demands judgment against Defendants as follows:

1. For general damages against Defendants, and each of them, jointly and severally, in an amount to be determined at trial, but in no event less than $24,000,000, less credits for any amounts recovered by Plaintiff from others;

2. For exemplary and punitive damages against Defendants, and each of them, in an amount to be determined at trial, but in no event greater than nine times the amount of general and special damages awarded to Plaintiff ($216 million);

3. For preliminary and permanent injunctive relief against Cross-Defendants, and each of them, enjoining and restraining them from continue to engage in unfair competition, unfair practices, violation of privacy, and other actions;

4. For a declaration that the Agreement in its entirety is unenforceable as unconscionable and against public policy or, in the alternative, that (a) the Exculpatory Provision is unenforceable as against Plaintiff; (b) the Damages Resolution is unenforceable against Plaintiff; and (c) the Indemnity is unenforceable against Mr. Terpin;

5. For attorney's fees under the FCA and any other applicable statutory provision;

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

6. For interest and costs of suit and such other and further relief as the Court deems just and proper.

DATED: March 16, 2020

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By:/s/Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a trial by jury.

DATED: March 16, 2020

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By:/s/ Pierce O'Donnell
PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590